




**The Deputy Secretary of Energy**  
Washington, DC 20585

December 7, 2009

**MEMORANDUM FOR UNDER SECRETARY FOR NUCLEAR SECURITY  
UNDER SECRETARY OF ENERGY  
UNDER SECRETARY FOR SCIENCE  
CHIEF INFORMATION OFFICER**

**FROM: DANIEL B. PONEMAN**   
**SUBJECT: Cyber Security Management**

Based on the decision of the Operations Management Council on November 5, 2009, and follow-up actions, I request that each of you do your part to implement the attached Department of Energy Cyber Security Governance Structure.

In addition, I request that you implement the additional cyber security actions that are listed in the attached Additional Cyber Security Management Actions document. These actions are drawn from the 60-day Cyber Review Team's report and from the recent cyber security study performed as part of the FY 2011 budget process.

**Attachments:**

1. Recommended Cyber Security Governance Structure
2. Additional Cyber Security Management Actions
3. DOE Cyber Security Data Protection Levels, with Examples

**cc: Chief Financial Officer**  
**Director, Office of Intelligence and Counterintelligence**

## DOE Cyber Security Governance Structure

DOE's cyber security governance recognizes that leadership of cyber security is a shared responsibility among the Under Secretaries and the Chief Information Officer. The actions identified below recognize the importance of involving the field in developing and reviewing proposed new or revised cyber security policy.

- Creation of a DOE Cyber Security Governance Council, consisting of the Under Secretaries and the Chief Information Officer *ex officio*, and chaired by one of the Under Secretaries. Each member will have the opportunity to have a staff member participate in Council meetings. The Director of the Office of Intelligence and Counterintelligence shall be an advisory member of the Council. The Council will:
  - Oversee development and management of DOE cyber security strategy, architecture, and program;
  - Assure that the DOE cyber security program is aligned with missions and the DOE management principles;
  - Guide DOE cyber security efforts to apply national standards and requirements, e.g., legislation, Office of Management and Budget (OMB) circulars and memoranda; Federal Information Processing Standards (FIPS) and guidance issued by the National Institute of Standards and Technology (NIST); and direction issued by the Committee on National Security Systems (CNSS).
  - Interact with and provide guidance to the Department's Chief Information Security Officer, who, by statute, leads DOE's cyber security program;
  - Consider broader issues of information technology (IT), Department-wide versus Program-specific platforms, and the role of the CIO, as appropriate.
- Creation of a DOE Cyber Security Advisory Group, consisting of one CIO representing the Science Laboratories, one CIO representing the NNSA Laboratories, one CIO representing the Energy Laboratories, and one CIO representing the NNSA Plants. This Advisory Group will:
  - Provide a disciplined and systematic approach for engaging key stakeholders to provide input for new or revised cyber security policy
  - Provide recommendations to the DOE Cyber Security Governance Council on the applicability, mission impact, risk, cost-benefit, and risk management of proposed new or revised cyber security directives

### **Additional Cyber Security Management Actions**

(Completion dates shown assume Deputy Secretary approval by November 20, 2009)

- Recognizing the Department's diverse mission objectives, involve DOE programs to jointly develop an enterprise level cyber security strategic plan for the Department to ensure alignment with DOE mission objectives. Action: Chief Information Security Officer (CISO) and Under Secretary representatives, with oversight by the DOE Cyber Security Governance Council (Council) (Completion of preliminary strategic plan by March 15, 2010)
- Establish a cyber security architecture framework, adaptable to the varied missions of the Department, to provide a common understanding of the secure design, implementation, and operations of the Department's information systems, and utilize to identify areas for common purchase agreements. Action: CISO and Under Secretary representatives, with oversight by the Council (Completion by May 31, 2010)
- Develop an enterprise training plan to provide a training strategy for the Department and determine ongoing resources needed to support an enterprise training program. Action: CISO and Under Secretary representatives, with oversight by the Council (Completion by January 31, 2010)
- Identify overlap in cyber security assessments, eliminate duplicative assessments where possible, and coordinate assessments with overlap in scope. Action: CISO, with oversight by the Council (Completion by March 31, 2010). Begin providing assessments as a common service to DOE organizations to enhance mission activities and support federal requirements. Action: CISO and Under Secretary representatives, with oversight by the Council (Completion by June 30, 2010)
- Set the baseline, or "minimum," requirements (those that are designed to apply to all DOE systems) to include NIST FIPS 199 and FIPS 200 for DOE unclassified systems. CNSS represents the baseline for classified systems. This is to include evaluation of the applicability, scope, and cost associated with additional baseline requirements derived from FIPS, OMB, FISMA, CNSS, and other authorities. This will provide a basis for protection of DOE data and systems in a graded manner, based on risk. Action: CISO and Under Secretary representatives, with oversight by the Council (Completion by April 15, 2010)
- Change the DOE Directives as follows:
  - Revise DOE O 205.1A, "Department of Energy Cyber Security Management," to be consistent with the Department's new management reform principles.
  - Review and revise the Incident Management manual to incorporate a risk-management approach.
  - Revise Media Sanitization and Process Requirements manuals to apply only to classified systems and media.

- Rescind remaining DOE cyber security manuals as they pertain to unclassified systems, and retain necessary content in the revision of DOE O 205.1A.  
Action: OCIO, through the CISO, with Under Secretary representatives, with oversight by the Council (Completion by June 30, 2010)
- Ensure that the FY 2012 budget development process addresses cyber security funding in a way that considers risk and that balances requirements with mission performance. Action: OCIO and CFO and the Programs (Completion by July 31, 2010)

## **DOE Cyber Security Data Protection Levels, with Examples**

The following hierarchical list of data protection levels, with examples of data at each level based on data sensitivity, is used to guide risk-based cyber security decisions. In general, the higher the level of sensitivity of data on a system, the more protection is appropriate.

### **Level 7 – Critical Assets**

- An example of a critical asset might be the digital file containing the complete detailed design description of a nuclear weapon component

### **Level 6 - CNSS<sup>1</sup> “High” Level**

- All Special Access Program (SAP) information, regardless of classification level
- All Sigma 14 and Sigma 20, regardless of classification level
- Top Secret Sensitive Compartmented Information (SCI)
- Top Secret and Secret RD (regardless of Sigma level), FRD, NSI
- DoD Critical Nuclear Weapons Design Information (CNWDI)
- North Atlantic Treaty Organization (NATO) COSMIC ATOMAL, Top Secret Atomic Principal
- Top Secret CRYPTO
- United Kingdom (UK) Top Secret (to include Atomic and Atomic Principal)

### **Level 5 - CNSS “Moderate” Level**

- Secret CRYPTO, SCI,
- NATO SECRET ATOMAL, Secret (Atomic Principal<sup>2</sup>), FRD , NSI
- Confidential RD
- Secret Naval Nuclear Propulsion Information (NNPI)

### **Level 4 - CNSS “Low” Level**

- NATO CONFIDENTIAL (to include Atomal)
- NATO RESTRICTED
- Confidential RD, FRD, NSI, CRYPTO, NNPI, FGI
- Safeguards Information (Nuclear Regulatory Commission)

### **Level 3 - FIPS<sup>2</sup> 199 *High* impact level**

- Unclassified Controlled Nuclear Information (UCNI)
- Confidential Foreign Government Information - Modified Handling Authorized (C/FGI-MOD)
- Export Controlled Information (ECI)
- Naval Nuclear Propulsion Information (NNPI)

---

<sup>1</sup> Committee on National Security Systems (CNSS), led by DOD. Just-released direction from CNSS actually calls for a more complex process to determine required protection levels, but this simplified three-level (Levels 4,5,and 6) listing for classified systems illustrates the generally stronger level of protection required for more sensitive information.

<sup>2</sup> Federal Information Processing Standard (FIPS), issued by NIST

**Level 2 - FIPS 199 *Moderate* impact level**

- UK Restricted
- Privacy Act information
- Sensitive Unclassified, e.g. Official Use Only (OUO), Limited Official Use (LOU), etc.
- Personally Identifiable Information (PII)
- Health Protected Information (HPI)
- Cooperative Research and Development Agreements (CRADA)
- Procurement/Business Sensitive Information
- Proprietary Information

**Level 1 - FIPS 199 *Low* impact level**

- Information produced in the Operations Security (OPSEC) process
- Law Enforcement Sensitive
- Unclassified Public and Non-Public Information

**Level 0 - FIPS 199 *Low* level**

- Fundamental research